

802.11a/n Outdoor Wireless CPE AP/Router

WNAP-7300

User's Manual

Version 1.0

Copyright

Copyright© 2011 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

FCC Caution

To assure continued compliance. (Example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

The availability of some specific channels and/or operational frequency bands are country

dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Energy Saving Note of the Device

This power required device does not support Stand by mode operation.

For energy saving, please press the power button or remove the DC-plug to disconnect the device from the power circuit. Without power off or remove the DC-plug, the device still consuming power from the power circuit. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to power off or remove the DC-plug for the device if this device is not intended to be active.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: except the channel 10 through 13, law prohibits the use of other channels.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of

WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual for PLANET 802.11a/n Outdoor Wireless CPE AP/Router

Model: WNAP-7300

Rev: 1.0 (January, 2011)

About This Manual

This user manual is intended to guide professional installer to install the WNAP-7300 and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:



• This indicates an important note that you must pay attention to.



• This indicates a warning or caution that you have to abide.

Bold: Indicates the function, important words, and so on.

Content

Chapter 1 Introduction	1
1.1 Introduction	1
1.2 Appearance	1
1.3 Key Features	2
1.4 Typical Application	2
Chapter 2 Hardware Installation	3
2.1 Preparation before Installation	3
2.1.1 Professional Installation Required	3
2.1.2 Safety Precautions	3
2.1.3 Installation Precautions	4
2.1.4 Product Package	4
2.2 Hardware Installation	6
2.2.1 Connect up	6
2.2.2 Using the External Antenna	10
2.2.3 Pole Mounting	11
Chapter 3 Basic Settings	13
3.1 Factory Default Settings	13
3.2 System Requirements	14
3.3 How to Login the Web-based Interface	14
3.4 Basic System Settings	17
3.5 Time Settings	20
3.6 RADIUS Settings	21
3.7 Firewall Settings	23
3.8 Basic Wireless Settings	27
3.9 Site Survey	30
Chapter 4 Advanced Settings	31
4.1 Advanced Wireless Settings	31
4.2 Wireless Security Settings	34
4.2.1 Security Settings	34

4.2.2 Access Control	36
4.2.3 WDS Settings	37
Chapter 5 Management	38
5.1 SNMP Management	38
5.1.1 Configure SNMPv3 User Profile	39
5.2 Upgrade Firmware	40
5.3 Backup/ Retrieve Settings	42
5.4 Restore Factory Default Settings	43
5.5 Reboot	43
5.6 Password	44
5.7 System Log	45
5.8 Site Survey	46
5.9 Ping Watch Dog	47
Chapter 6 Status	49
6.1 View Basic Information	49
6.2 View Association List	50
6.3 View Network Flow Statistics	50
6.4 View ARP Table	52
6.5 View Bridge Table	52
6.6 View Active DHCP Client Table	53
Chapter 7 Troubleshooting	54
Appendix A. ASCII	56
Appendix B. GPL Declamation	57

FIGURE

Figure 1 WNAP-7300	1
Figure 2 Typical Application	2
Figure 3 Move the Cover	3
Figure 4 Cable Connection	3
Figure 5 Enable the Secondary RJ45 Power	7
Figure 6 Power on the device by PWR button	7
Figure 7 Attach and fasten the removable cover	3
Figure 8 Connect to POE Injector	3
Figure 9 Complete Set	9
Figure 10 Remove the plugs	С
Figure 11 Connect to external antenna	Э
Figure 12 Pole Mounting – Step 111	1
Figure 13 Pole Mounting – Step 2	2
Figure 14 Login Page	5
Figure 15 Main Page	6
Figure 16 Basic System Settings	7
Figure 17 TCP/IP Settings (Bridge)	3
Figure 18 TCP/IP Settings (Router)	9
Figure 19 Time Settings	1
Figure 20 RADIUS Settings	2
Figure 21 Source IP Filtering	3
Figure 22 Destination IP Filtering24	4
Figure 23 Source Port Filtering	4
Figure 24 Destination Port Filtering	5
Figure 25 Port Forwarding	6
Figure 26 DMZ	3
Figure 27 Basic Wireless Settings	7
Figure 28 Site Survey	Э
Figure 29 Advanced Wireless Settings	1
Figure 30 Security Settings	4
Figure 31 Access Control	a

Figure 32 WDS Settings	37
Figure 33 SNMP Configuration	38
Figure 34 Configure SNMPv3 User Profile	39
Figure 35 Upgrade Firmware	41
Figure 36 Backup/Retrieve Settings	42
Figure 37 Restore Settings	43
Figure 38 Reboot	44
Figure 39 Password	45
Figure 40 System Log	46
Figure 41 Site Survey Tool	47
Figure 42 Ping Watchdog	47
Figure 43 Basic Information	49
Figure 44 Connection	50
Figure 45 Network Flow Statistics	51
Figure 46 ARP Table	52
Figure 47 Bridge Table	53
Figure 48 DHCP Client Table	53

TABLE

Table 1 Factory Default Settings	. 13
Table 2 ACSII	57
Table 3 Public Software Name and Description	59

Chapter 1 Introduction

1.1 Introduction

Designed for outdoor environment application, the WNAP-7300 is a high-performance 802.11a/n 2x2 MIMO broadband solution that provides fast and reliable wireless network coverage. Designed with IEEE 802.11n standard, high output power and built-in 16dBi dual-polarity antenna makes it possible to deliver several times faster data rate than normal wireless device and higher bandwidth with longer range for outdoor applications.

The WNAP-7300 supports four wireless communication connectivity (AP, Wireless Client, WDS and AP+WDS), allowing for various application requirements thus helping to find the key to the "last mile" with least effort.

With high output power and reliable performance, the WNAP-7300 is an ideal wireless broadband solution for wireless Internet service providers and system integrators!

1.2 Appearance



Figure 1 WNAP-7300

1.3 Key Features

- Compliant with IEEE 802.11a and IEEE 802.11n as well
- Support Power through Ethernet which is supplied with 15V.
- High reliable watertight housing endures almost any harsh environments
- Four operating modes including AP, Wireless Client, WDS and AP+WDS
- Support 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and
 WPA-PSK&WPA2-PSK etc
- User-friendly Web and SNMP-based management interface

1.4 Typical Application

This section describes the typical applications of the WNAP-7300. By default, it is set to AP mode which allows it to establish a wireless coverage; besides, it is also able to join any available wireless network under wireless client mode. The WNAP-7300 is able to deliver stable and efficient broadband connectivity for various applications.

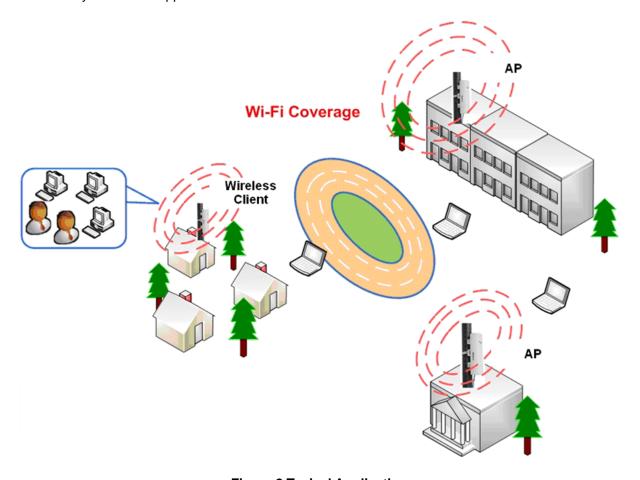


Figure 2 Typical Application

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing the WNAP-7300.

2.1 Preparation before Installation

2.1.1 Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

2.1.2 Safety Precautions

- To keep you safe and install the hardware properly, please read and follow these safety precautions.
- If you are installing the WNAP-7300 for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
- Keep safety as well as performance in mind when selecting your installation site, especially
 where there are electric power and phone lines.
- 4. When installing the WNAP-7300, please note the following things:
 - Do not use a metal ladder;
 - Do not work on a wet or windy day;
 - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
- 5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

2.1.3 Installation Precautions

To keep the WNAP-7300 well while you are installing it, please read and follow these installation precautions.

- Users MUST use a proper and well-installed surge arrestor with the WNAP-7300; otherwise, a random lightening could easily cause fatal damage to the unit. EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.
- Users MUST use the "Power cord & POE Injector" shipped in the box with the WNAP-7300.
 Use of other options will cause damage to the unit.
- Users MUST power off the WNAP-7300 first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the WNAP-7300; otherwise, damage might be caused to the device itself.

2.1.4 Product Package

The product package you have received should contain the following items:

•	The WNAP -7300	x 1
•	Pole Mounting Ring	x 2
•	PoE Injector	x 1
•	Power Adapter	x 1
•	Quick Installation Guide (QIG)	x 1
•	Product CD (User's Manual & QIG included)	x 1

Note:

• If any of them are not included or damaged, please contact your local vendor for support.

Pole Mounting Ring



Power Adapter & POE Injector





 Users MUST use the "Power Adapter & POE Injector" shipped in the box with the WNAP-7300. Use of other options will cause damage to the unit.

2.2 Hardware Installation

2.2.1 Connect up

The bottom of WNAP-7300 is a movable cover. Loosen the screw with a Phillips screwdriver.
 Grab the cover and pull it out as the figure shown below.

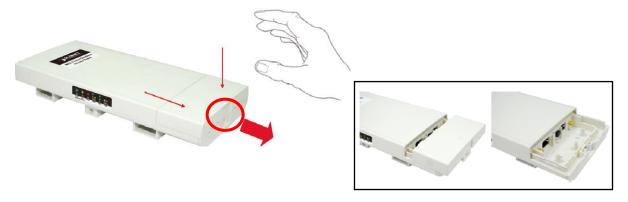


Figure 3 Move the Cover

 Plug a standard Ethernet cable into the RJ45 port labeled "LAN 1". Do not plug the cable into the RJ45 port labeled "LAN 2".



Figure 4 Cable Connection

** The secondary Ethernet port (labeled LAN 2) is for IP video integration. To use it you need to enable the secondary port in advance before connecting with the IP camera from the WNAP-7300's Web Management as shown below.

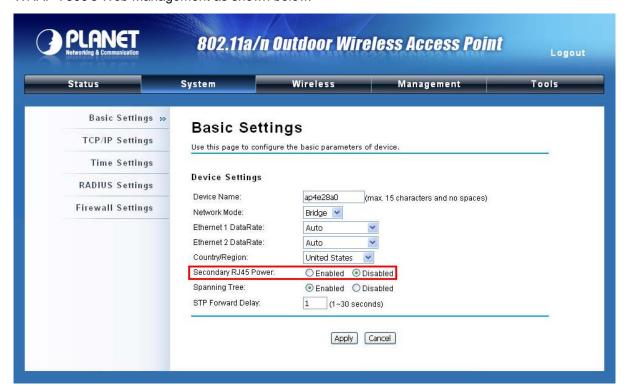


Figure 5 Enable the Secondary RJ45 Power

3. Press the black PWR button beside the LAN 1 Ethernet port.



Figure 6 Power on the device by PWR button

4. Attach and fasten the removable cover to the bottom of the WNAP-7300. When finished, you can check the connection as the figure shown below.



Figure 7 Attach and fasten the removable cover

5. Plug the power cord into the DC port of the POE injector as the figure shown below.



Figure 8 Connect to POE Injector

6. Plug the other side of the Ethernet cable in the Step.4 into the POE port of the POE injector in the Step.5, and get the complete set ready as the figure shown below.



Figure 9 Complete Set

Note:

- Be reminded, the UTP wire distance toward your WNAP-7300 to the Ethernet devices, such as Ethernet Switch, is 100 meters, the passive POE injector can be in any point of this 100 meters UTP distance where there is a shell or protected location.
- 7. Power on the WNAP-7300 by plugging the power adapter to the power socket.

2.2.2 Using the External Antenna

The WNAP-7300 provides two reverse SMA antenna connectors if you prefer to use the external antenna for your application instead of the built-in directional antenna, please follow the steps below.

1. Remove the two plugs as circled below:



Figure 10 Remove the plugs

2. Connect your external antenna to the SMA-type connectors at the bottom of the WNAP-7300.

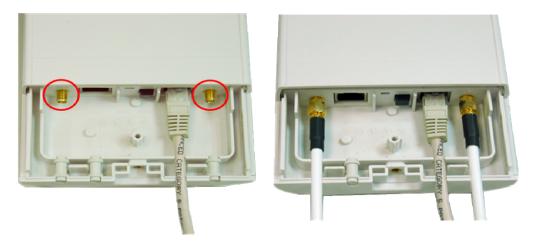


Figure 11 Connect to external antenna



Users MUST power off the WNAP-7300 first before connecting the external antenna to
it. Do not switch from built-in antenna to the external antenna from WEB management
without physically attaching the external antenna onto the WNAP-7300; otherwise,
damage might be caused to the unit itself.

Follow the steps described in **Connect Up** to finish the installation.

2.2.3 Pole Mounting

Turn the WNAP-7300 over. Put the pole mounting rings through the middle hole of it. Note that
you should unlock the pole mounting ring with a screw driver before putting it through the
WNAP-7300 as the following right picture shows.



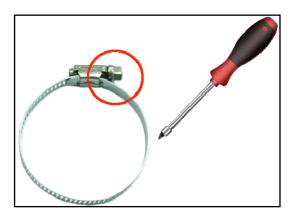


Figure 12 Pole Mounting - Step 1

2. Mount the WNAP-7300 steadily to the pole by locking the pole mounting ring tightly. The mounting ring supports pole diameter 32mm to 70mm.



Figure 13 Pole Mounting – Step 2

3. Now you have completed the hardware installation of the WNAP-7300.Basic Settings

Chapter 3 Basic Settings

3.1 Factory Default Settings

We'll elaborate the WNAP-7300 factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Table 1 Factory Default Settings

Features	;	Factory Default Settings
Usernam	е	admin
Password	b	admin
Wireless	Device Name	apXXXXXX (X represents the last 6
		digits of Ethernet MAC address)
Operating	g Mode	AP
Data Rat	е	Auto
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
LAN	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
Spanning	Tree	Enable
802.11 Mode		802.11a/n
Country/Region		United States
Channel Number		149
SSID		Wireless
Broadcast SSID		Enable
HT Protect		Disable
Data Rate		Auto
Output Power		100% (Full)
Channel	Mode	20MHz
WMM		Enabled
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Beacon Interval		100
DTIM Interval		1
Space in Meter		0
Flow Control by AP		Disable
Security		Open System
Encryption		None

Wireless Separation		Disable
Access Control		Disable
	Enable/Disable	Enable
SNMP	Read Community Name	Public
SINIVIE	Write Community Name	Private
	IP Address	0.0.0.0

3.2 System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of the WNAP-7300 is **192.168.1.1**. (X cannot be 0, 1, nor 255);
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above,
 Netscape or Firefox.

3.3 How to Login the Web-based Interface

The WNAP-7300 provides you with user-friendly Web-based management tool.

 Open Web browser and enter the IP address (Default: 192.168.1.1) of the WNAP-7300 into the address field. You will see the login page as below.



Figure 14 Login Page

Enter the username (Default: admin) and password (Default: admin) respectively and click "Login" to login the main page of the WNAP-7300. As you can see, this management interface provides six main options in the black bar above, which are Status, System, Wireless, Management and Tools.



Figure 15 Main Page

Note:

 The username and password are case-sensitive, and the password should be no more than 19 characters!

3.4 Basic System Settings

For users who use the WNAP-7300 for the first time, it is recommended that you begin configuration from "Basic Settings" in "System" shown below:

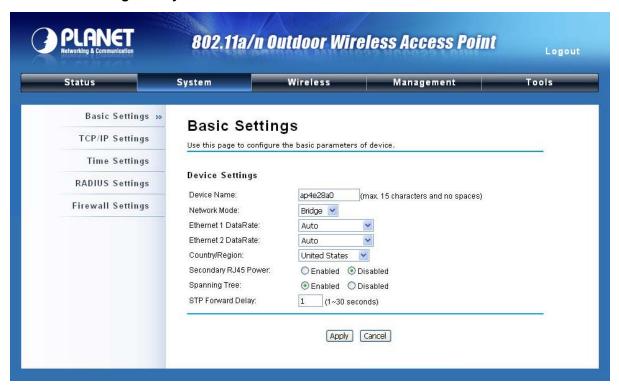


Figure 16 Basic System Settings

Basic Settings

Device Name: Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

Network Mode: Specify the network mode, including Bridge and Router. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the device when it is set to Router Mode. For details, please refer to "**IP Settings (Router)**".

Ethernet 1 Data Rate: Specify the transmission rate of data of LAN1. Default is **Auto**.

Ethernet 2 Data Rate: Specify the transmission rate of data of LAN2. Default is **Auto**.

<u>Country Region</u>: The availability of some specific channels and/or operational frequency bands are country dependent.

<u>Secondary RJ45 Power</u>: The secondary Ethernet port (labeled LAN 2) is for IP video integration. To use it you need to enable the secondary port via WEB UI in advance before connecting with the IP camera.

Spanning Tree: Spanning Tree Protocol (STP) is a link management protocol for AP which

provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

STP Forward Delay: STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. Default time value is 1 sec.

TCP/IP Settings

Open "TCP/IP Settings" in "System" as below to configure the parameters for LAN which connects to the LAN port of the WNAP-7300. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.

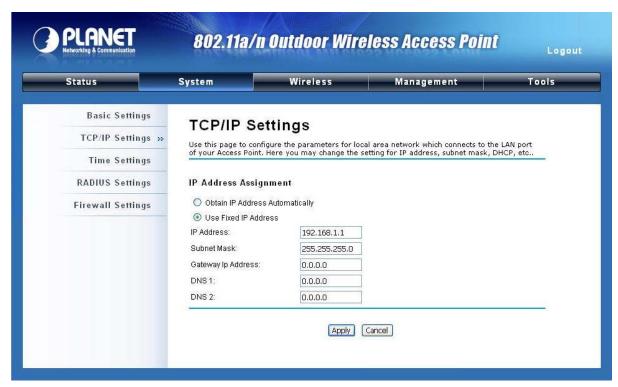


Figure 17 TCP/IP Settings (Bridge)

<u>Obtain IP Address Automatically</u>: If a DHCP server exists in your network, you can check this option, thus the WNAP-7300 is able to obtain IP settings automatically from that DHCP server.



• When the IP address of the WNAP-7300 is changed, the clients on the network often need to wait for a while or even reboot before they can access the new IP address. For an immediate access to the bridge, please flush the netbios cache on the client computer by running the "nbtstat –r" command before using the device name of the WNAP-7300 to access its Web Management page.

<u>Use Fixed IP Address</u>: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for the WNAP-7300 manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

If the WNAP-7300 is configured as Router mode, you need to configure some additional TCP/IP parameters for accessing the Internet.



Figure 18 TCP/IP Settings (Router)

<u>WAN Settings</u>: Specify the Internet access method to Static IP, DHCP or PPPOE. Users must enter WAN IP Address, Subnet Mask, Gateway settings provided by your ISPs.

LAN Settings: When DHCP Server is disabled, users can specify IP address and subnet mask for the WNAP-7300 manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range, DHCP Subnet Mask, DHCP Gateway and Lease Time (15-44640 minutes).

A Warning:

- In AP mode, the WNAP-7300 must establish connection with another wireless device before it is set to Router mode. In Router mode, it is impossible for users to access device via wired port, for WAN is on wired port and LAN is on wireless port. Users can access device through the wireless device connected with the WNAP-7300.
- In wireless client mode, users can access the WNAP-7300 via its wired port, for WAN
 is on wireless port and LAN is on wired port when device is set to Router mode.
- Bridge mode and AP+Bridge mode are similar to AP mode when device is set to Router mode; WAN is on wired port and LAN is on wireless port. Thus users must also connect the WNAP-7300 with another wireless device before it is set to Router mode and access the WNAP-7300 via the connected wireless device.

3.5 Time Settings

Compliant with NTP, the WNAP-7300 is capable of keeping its time in complete accord with the Internet time. Make configuration in "Time Settings" from "System". To use this feature, check "Enable NTP Client Update" in advance.



Figure 19 Time Settings

Current Time

Display the present time in Yr, Mon, Day, Hr, Min and Sec.

Time Zone Select

Select the time zone from the dropdown list.

NTP Server

Select the time server from the "NTP Server" dropdown list or manually input the IP address of available time server into "Manual IP".

Hit "Apply" to save settings.

3.6 RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.

Open "RADIUS Settings" in "System" to make RADIUS configuration.

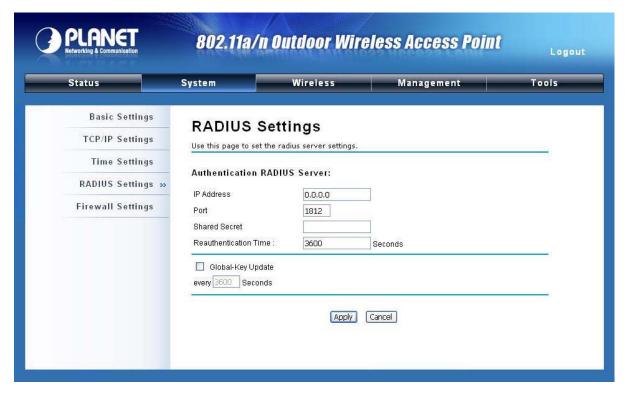


Figure 20 RADIUS Settings

Authentication RADIUS Server

This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

IP Address: Enter the IP address of the Radius Server;

Port: Enter the port number of the Radius Server;

Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the AP and RADIUS during authentication.

Re-authentication Time: Set the time interval between two authentications.

<u>Global-Key Update</u>: Check this option and specify the time interval between two global-key updates.

3.7 Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. The WNAP-7300 has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under Router Mode.

Source IP Filtering: The source IP filtering gives users the ability to restrict certain types of data packets from your local network to Internet through the WNAP-7300. Use of such filters can be helpful in securing or restricting your local network.



Figure 21 Source IP Filtering

<u>Destination IP Filtering</u>: The destination IP filtering gives you the ability to restrict the computers in LAN from accessing certain websites in WAN according to specified IP addresses. Check the "Enable Destination IP Filtering" checkbox and enter the IP address of the clients to be restricted. Hit Apply to make the setting take effect.



Figure 22 Destination IP Filtering

Source Port Filtering: The source port filtering enable you to restrict certain ports of data packets from your local network to Internet through the WNAP-7300. Use of such filters can be helpful in securing or restricting your local network.

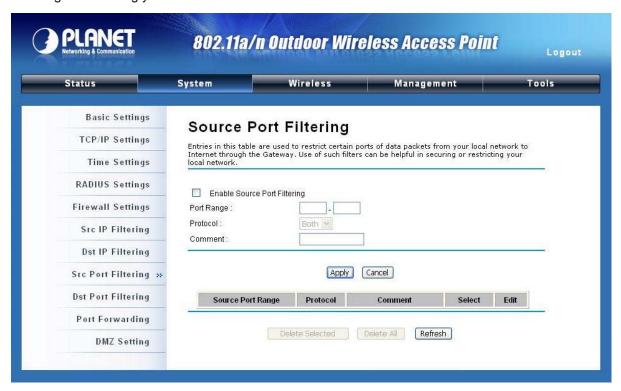


Figure 23 Source Port Filtering

Destination Port Filtering: The destination port filtering enables you to restrict certain ports of data

packets from your local network to Internet through the WNAP-7300. Use of such filters can be helpful in securing or restricting your local network.



Figure 24 Destination Port Filtering

Port Forwarding: The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings ne are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind the router's NAT firewall.



Figure 25 Port Forwarding

<u>DMZ</u>: A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to the Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



Figure 26 DMZ

3.8 Basic Wireless Settings

Open "Basic Settings" in "Wireless" as below to make basic wireless configuration.

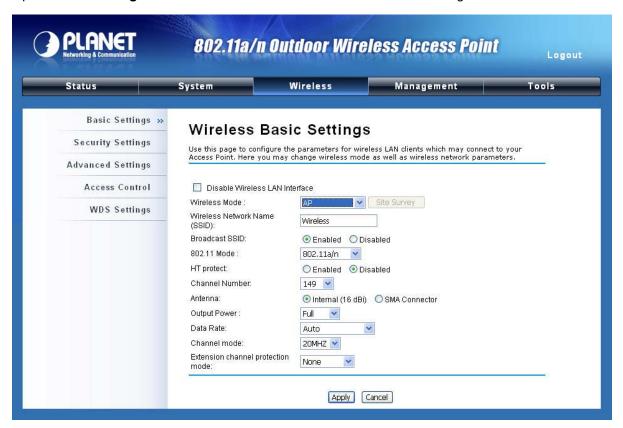


Figure 27 Basic Wireless Settings

Disable Wireless LAN Interface

Check this option to disable WLAN interface, then the wireless module of the WNAP-7300 will stop working and no wireless device can connect to it.

Wireless Mode

Four operating modes are available on the WNAP-7300.

<u>AP</u>: The WNAP-7300 establishes a wireless coverage and receives connectivity from other wireless devices.

<u>Wireless Client</u>: The WNAP-7300 is able to connect to the AP and thus join the wireless network around it.

Bridge: The WNAP-7300 establishes wireless connectivity with other APs by keying in remote MAC address. Please refer to the "WDS Setting" for detailed configuration.

<u>AP+Bridge</u>: The WNAP-7300 servers as AP and Bridge concurrently. In other words, it can provide connectivity services for WNAP-7300s under WDS mode.

Wireless Network Name (SSID)

This wireless network name is shared among all associated devices in your wireless network.

Keep it identical on all those devices. Note that the SSID is case-sensitive and cannot exceed 32 characters.

Broadcast SSID

In AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA cannot scan and find the WNAP-7300, so that malicious attack by some illegal STA could be avoided.

802.11 Mode

The WNAP-7300 can communicate with wireless devices of 802.11n or 802.11a/n. You can also select Auto and make it work under an appropriate wireless mode automatically.

HT Protect

Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

Channel Number

Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

Antenna

By default, the WNAP-7300 uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (16 dBi)" to "SMA Connector".

Note:

You are able to choose "SMA Connector" only from the WEB UI when you have well
done installing the external antenna; otherwise, it might damage the unit itself.

Output Power

Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. Usually "Full" is preferred.

Data Rate

Usually "Auto" is preferred. Under this rate, the Wireless Outdoor WNAP-7300 will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

Channel Mode

Four levels are available: 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

Extension Channel Protection Mode

This is to avoid conflict with other wireless network and boost the ability of your device to catch all legacy devices transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Enable MAC Clone

Available only under wireless client mode, it hides the MAC address of the WNAP-7300 while displays the one of associated wireless client or the MAC address designated manually.

3.9 Site Survey

Under wireless client mode, the WNAP-7300 is able to perform site survey, through which, information on the available access points will be detected.

Open "Basic Settings" in "Wireless", by clicking the "Site Survey" button beside "Wireless Mode" option, the wireless site survey window will pop up with a list of available wireless networks around. Select the AP you would like to connect and click "Selected" to establish connection. The wireless site survey window can also be viewed by opening the "Site Survey" page in "Tools".

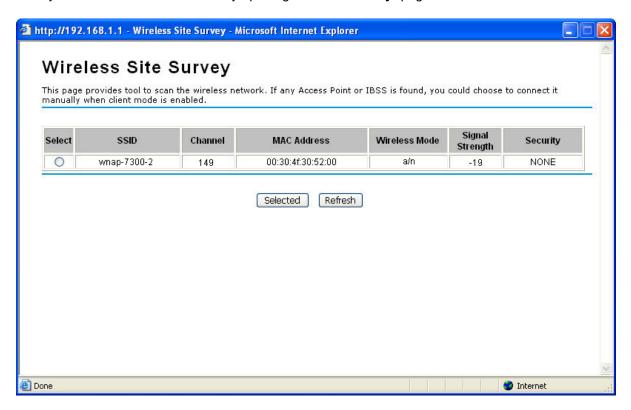


Figure 28 Site Survey

Chapter 4 Advanced Settings

4.1 Advanced Wireless Settings

Open "Advanced Settings" in "Wireless" to make advanced wireless settings.



Figure 29 Advanced Wireless Settings

WMM Support

WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it.

A-MPDU/A-MSDU Aggregation

The data rate of your WNAP-7300 except wireless client mode could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is not recommended to enable it.

Short GI

Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

RTS Threshold

The WNAP-7300 sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Fragmentation Length

Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Beacon Interval

Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

DTIM Interval

DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

IGMP Snooping

IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

Wireless Separation

Wireless separation is an ideal way to enhance the security of network transmission. Under the mode except wireless client mode, enable "Wireless Separation" can prevent the communication among associated wireless clients.

RIFS

RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency.

Link Integration

Available under AP/Bridge/AP+Bridge mode, it monitors the connection on the Ethernet port by checking "**Enabled**". It can inform the associating wireless clients as soon as the disconnection occurs.

Max. Station Num

Available only under AP mode, it defines the maximum amount of wireless clients allowed to be connected.

Space in Meter/ACK Timeout

To decrease the chances of data retransmission at long distance, the WNAP-7300 can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

Flow Control

It allows the administrator to specify the incoming and outgoing traffic limit by checking "Enable Traffic Shaping". This is only available in Router mode.

Note:

We strongly recommend you leave most advanced settings at their defaults except
 "Distance in Meters" adjusted the parameter for real distance; any modification on them may negatively impact the performance of your wireless network.

4.2 Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, the WNAP-7300 provides you with rock solid security settings.

4.2.1 Security Settings

Open "Security Settings" in "Wireless" as below:



Figure 30 Security Settings

Network Authentication

Open System: It allows any device to join the network without performing any security check.

Shared Key: Data encryption and key are required for wireless authentication.

<u>Legacy 802.1x</u>: As an IEEE standard for port-based Network Access Control, it provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.

<u>WPA with RADIUS</u>: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

WPA2 with RADIUS: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, AES encryption and RADIUS server is required.

<u>WPA&WPA2 with RADIUS</u>: It provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.

<u>WPA-PSK</u>: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

<u>WPA-PSK&WPA2-PSK</u>: It provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

Data Encryption

If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers.

128 bits WEP: It is made up of 26 hexadecimal numbers.

152 bits WEP: It is made up of 32 hexadecimal numbers.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: It allows for backwards compatibility with devices using TKIP.



- We strongly recommend you enable wireless security on your network!
- Only setting the same Authentication, Data Encryption and Key in the WNAP-7300 and other associated wireless devices, can the communication be established!

4.2.2 Access Control

The Access Control appoints the authority to wireless client on accessing the WNAP-7300, thus a further security mechanism is provided. This function is available only under AP mode.

Open "Access Control" in "Wireless" as below.



Figure 31 Access Control

Access Control Mode

If you select "Allow Listed", only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when "Deny Listed" is selected, those wireless clients on the list will not be able to connect the AP.

MAC Address

Enter the MAC address of the wireless client that you would like to list into the access control list, click "Apply" then it will be added into the table at the bottom.

Delete Selected/All

Check the box before one or more MAC addresses of wireless client(s) that you would like to cancel, and click "Delete Selected" or "Delete All" to cancel that access control rule.

4.2.3 WDS Settings

Extend the range of your network without having to use cables to link the bridges by using the Wireless Distribution System (WDS): Simply put, you can link the bridges wirelessly. Open "WDS Settings" in "Wireless" as below:



Figure 32 WDS Settings

Enter the MAC address of another WNAP-7300 you wirelessly want to connect to into the appropriate field and click "**Apply**" to save settings.



• WDS Settings is available only under Bridge and AP+Bridge Mode.

Chapter 5 Management

5.1 SNMP Management

The WNAP-7300 supports SNMP for convenient remote management. Open "SNMP Configuration" in "Management" shown below. Set the SNMP parameters and obtain MIB file before remote management.



Figure 33 SNMP Configuration

Enable SNMP

Check this box to enable SNMP settings.

Protocol Version

Select the SNMP version, and keep it identical on the WNAP-7300 and the SNMP manager.

Server Port

Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

Get Community

Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

Set Community

Specify the password for the incoming Set requests from the management station. By default, it is set to private.

Trap Destination

Specify the IP address of the station to send the SNMP traps to.

Trap Community

Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

5.1.1 Configure SNMPv3 User Profile

For SNMP protocol version 3, you can click "Configure SNMPv3 User Profile" in blue to set the details of SNMPv3 user. Check "Enable SNMPv3 Admin/User" in advance and make further configuration.

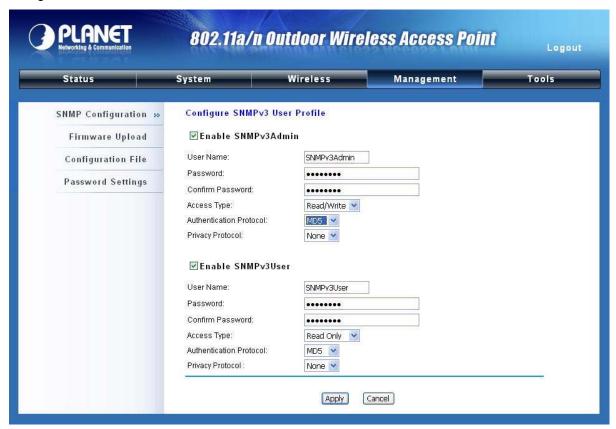


Figure 34 Configure SNMPv3 User Profile

User Name

Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the WNAP-7300.

Password

Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the WNAP-7300.

Confirm Password

Input that password again to make sure it is your desired one.

Access Type

Select "Read Only" or "Read and Write" accordingly.

Authentication Protocol

Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

Privacy Protocol

Specify the encryption method for SNMP communication. None and DES are available.

None: No encryption is applied.

DES: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

5.2 Upgrade Firmware

Open "Firmware Upload" in "Management" and follow the steps below to upgrade firmware locally or remotely through the WNAP-7300's Web:



Figure 35 Upgrade Firmware

- Click "Browse" to select the firmware file you would like to load;
- Click "Upload" to start the upload process;
- Wait a moment, the system will reboot after successful upgrade.

Note:

• Do NOT cut the power off during upgrade, otherwise the system may crash!

5.3 Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open "Configuration File" in "Management" as below:



Figure 36 Backup/Retrieve Settings

Save Settings to File

By clicking "Save", a dialog box will pop up. Save it, then the configuration file like ap.cfg will be saved to your local computer.

Load Setting from File

By clicking "Browse", a file selection menu will appear, select the file you want to load, like ap.cfg; Click "Upload" to load the file. After automatically rebooting, new settings are applied.

5.4 Restore Factory Default Settings

The WNAP-7300 provides two ways to restore the factory default settings:

Restore factory default settings via Web

From "Configuration File", clicking "Reset Settings to Default" will eliminate all current settings and reboot your device, then default settings are applied.

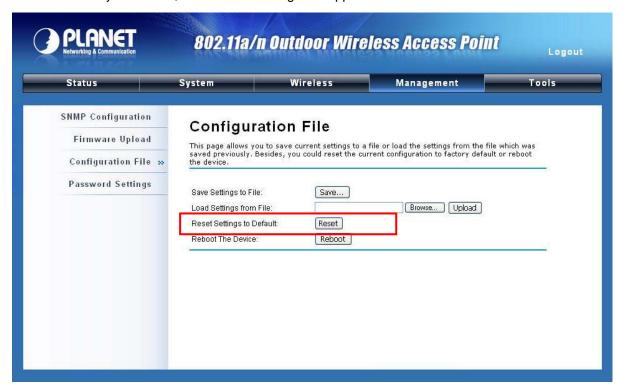


Figure 37 Restore Settings

Restore factory default settings via Reset Button

If software in the WNAP-7300 is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least 5 seconds and then release it until the PWR LED gives a blink.

5.5 Reboot

You can reboot your WNAP-7300 from "Configuration File" in "Management" as below:

Click "Reboot" and hit "Yes" upon the appeared prompt to start reboot process. This takes a few minutes.



Figure 38 Reboot

5.6 Password

From "Password Settings" in "Management", you can change the password to manage your WNAP-7300.

Enter the new password respectively in "New Password" and "Confirm Password" fields; click "Apply" to save settings.



Figure 39 Password



• The password is case-sensitive and its length cannot exceed 19 characters!

5.7 System Log

System log is used for recording events occurred on the WNAP-7300, including station connection, disconnection, system reboot and etc.

Open "System Log" in "Tools" as below.



Figure 40 System Log

Remote Syslog Server

Enable Remote Syslog: Enable System log to alert remote server.

IP Address: Specify the IP address of the remote server.

Port: Specify the port number of the remote server.

5.8 Site Survey

Only available under Wireless Client mode, site survey allows you to scan all the APs within coverage.

Open "Site Survey" in "Tools" as below and select the desired AP to connect.



Figure 41 Site Survey Tool

5.9 Ping Watch Dog

If you mess your connection up and cut off your ability the log in to the unit, the ping watchdog has a chance to reboot due to loss of connectivity.



Figure 42 Ping Watchdog

Ping Watchdog

<u>Enable Ping Watchdog</u>: To activate ping watchdog, check this checkbox.

<u>IP Address to Ping</u>: Specify the IP address of the remote unit to ping.

<u>Ping Interval</u>: Specify the interval time to ping the remote unit.

Startup Delay: Specify the startup delay time to prevent reboot before the WNAP-7300 is fully initialized.

Failure Count To Reboot: If the ping timeout packets reached the value, the WNAP-7300 will reboot automatically.

Chapter 6 Status

6.1 View Basic Information

Open "Information" in "Status" to check the basic information of the WNAP-7300, which is read only. Click "Refresh" at the bottom to have the real-time information.



Figure 43 Basic Information

6.2 View Association List

Open "Association List" in "Connection" from "Status" to check the information of associated wireless clients. All is read only. Click "Refresh" at the bottom to view the current association list.

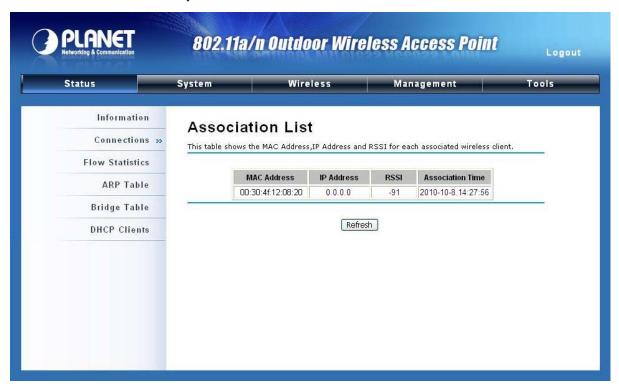


Figure 44 Connection

6.3 View Network Flow Statistics

Open "Flow Statistics" in "Status" to check the data packets received on and transmitted from the wireless and Ethernet ports. Click "Refresh" to view current statistics.

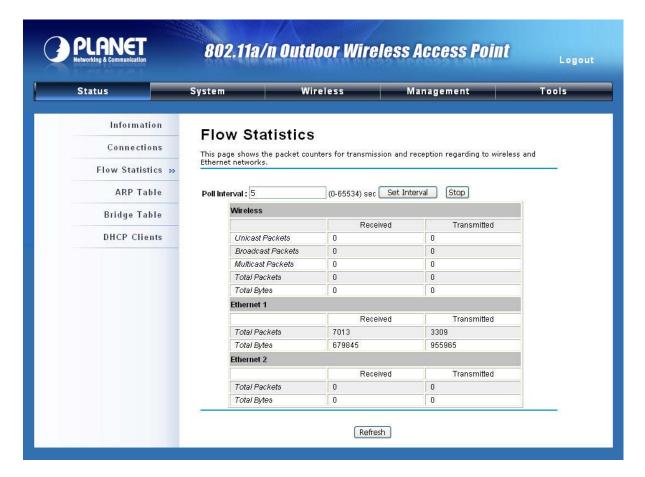


Figure 45 Network Flow Statistics

Poll Interval

Specify the refresh time interval in the box beside "**Poll Interval**" and click "**Set Interval**" to save settings. "**Stop**" helps to stop the auto refresh of network flow statistics.

6.4 View ARP Table

Open "ARP Table" in "Status" as below. Click "Refresh" to view current table.



Figure 46 ARP Table

6.5 View Bridge Table

Open "Bridge Table" in "Status" as below. Click "Refresh" to view current connected status.



Figure 47 Bridge Table

6.6 View Active DHCP Client Table

Open "DHCP Client List" in "Status" as below to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click "Refresh" to view current table.



Figure 48 DHCP Client Table

Chapter 7 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the WNAP-7300. For warranty assistance, contact your service provider or distributor for the process.

Q 1. How to know the MAC address of the WNAP-7300?

MAC Address distinguishes itself by the unique identity among network devices. There are two ways available to know it.

- Each device has a label posted with the MAC address which located in the back of the device.
- On the WNAP-7300's Web-based management interface, you can view the MAC Address from "View Basic Information".

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in "Configuration File" from "Management".

Q 3. What if I would like to backup and retrieve my configuration settings?

You may do the backup by generating a configuration file or retrieve the settings you have backed up previously in "Configuration File" from "Management".

Q 4. What if I can not access the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.
- Check whether the IP address of PC is correct (in the same network segment as the unit);
- Login the unit via other browsers such as Firefox.
- Hardware reset the unit.

Q 5. In wireless client mode, what if the wireless connection is not stable after associating with an AP?

- Since the WNAP-7300 comes with a built-in directional antenna, it is recommended make it
 face to the direction where the AP is to get the best connection quality.
- In addition, you can start "Site Survey" in "Wireless Basic Settings" to check the signal strength. If it is weak or unstable (The smaller the number is, the weaker the signal strength is.), please join other available AP for better connection.

Appendix A. ASCII

WEP can be configured with a 64-bit, 128-bit or 152-bit Shared Key (hexadecimal number or ACSII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

Table 2 ACSII

ASCII	Hex	ASCII	Hex	ASCII	Hex	ASCII	Hex
Character	Equivalent	Character	Equivalent	Character	Equivalent	Character	Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
\$	24	<	3C	Т	54	I	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
•	27	?	3F	W	57	0	6F
(28	@	40	Χ	58	р	70
)	29	Α	41	Υ	59	q	71
*	2A	В	42	Z	5A	r	72
+	2B	С	43	[5B	S	73
,	2C	D	44	\	5C	t	74
-	2D	E	45]	5D	u	75
	2E	F	46	۸	5E	V	76
/	2F	G	47	_	5F	W	77
0	30	Н	48	`	60	Х	78
1	31	1	49	а	61	у	79
2	32	J	4A	b	62	Z	7A
3	33	K	4B	С	63	{	7B
4	34	L	4C	d	64	1	7C
5	35	М	4D	е	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	0	4F	g	67		
8	38	Р	50	h	68		

Appendix B. GPL Declamation

PUBLIC SOFTWARE DECLAMATION

In the software we delivered, there may contains some public software, if it is, please read below carefully:

1. Definition

"Public Software", when applicable, shall mean that portion of the Licensed Software, in source code form, set forth in the below Table, and provided under the terms set forth in the Section 5, the indicated website, the complete license terms can be found.

"Public Software" shall mean each of:

- (a) any computer code that contains, or is derived in any manner (in whole or in part) from, any computer code that is distributed as open source software (e.g. Linux) or similar licensing or distribution models; and
- (b) any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software (i) be disclosed or distributed in source code form, (ii) be licensed for the purpose of making derivative works, or (iii) be redistributable at no charge.

Public Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (1) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (2) the Artistic License (e.g., PERL); (3) the Mozilla Public License; (4) the Netscape Public License; (5) the Sun Community Source License (SCSL); (6) the Sun Industry Source License (SISL); and (7) the Apache Software license.

2. Limited Use

Any Public Software provided under the agreement shall be subject to the licenses, terms and conditions of its model. Licensee hereby agrees to comply with the terms and conditions applicable to any such Public Software, as set forth in its presentation on website.

3. Limited Liability

The supplier hereby express that the supplier shall have no liability for any costs, loss or damages resulting from Licensee's breach of the terms and conditions applicable to use, conversion or combination of the licensed software with or into Public Software.

4. NO WARRANTY

This program or licensed software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY. THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH LICENSEE.

5. Public Software Name and Description

Table 3 Public Software Name and Description

Program	Copy Right	Origin Sour	Licenses or	License Terms
Name	Description	Code	Distribution Models or	Website
			its special license	Reference
			terms	
U-boot	Wolfgang Denk,	ftp://ftp.denx.de/	GNU GENERAL	GNU GENERAL
	DENX Software	pub/u-boot/	PUBLIC LICENSE	PUBLIC
	Engineering,		Version 2	LICENSE Version
	wd@denx.de			2
Busybox		http://www.busy	GNU GENERAL	http://www.gnu.or
		box.net/downloa	PUBLIC LICENSE	g/licenses/old-lice
		ds/busybox-1.01	Version 2	nses/gpl-2.0.html
		.tar.bz2		
Goahead	Copyright (c)	http://data.goahe		
	GoAhead Software	ad.com/Software		
	Inc., 1992-2000.	/Webserver/2.1.		
		8/webs218.tar.gz		

hostapd	Copyright (c)	http://hostap.epit	GNU GENERAL	http://www.gnu.or
	2002-2006, Jouni	est.fi/releases/h	PUBLIC LICENSE	g/licenses/old-lice
	Malinen	ostapd-0.4.8.tar.	Version 2	nses/gpl-2.0.html
	<jkmaline@cc.hut.fi< td=""><td>gz</td><td></td><td></td></jkmaline@cc.hut.fi<>	gz		
	> and			
	contributors			
wpa_sup	Copyright (c)	http://hostap.epit	GNU GENERAL	http://www.gnu.or
plicant	2003-2005, Jouni	est.fi/releases/w	PUBLIC LICENSE	g/licenses/old-lice
	Malinen	pa_supplicant-0.	Version 2	nses/gpl-2.0.html
	<jkmaline@cc.hut.fi< td=""><td>4.7.tar.gz</td><td></td><td></td></jkmaline@cc.hut.fi<>	4.7.tar.gz		
	> and			
	contributors			
ntpclient	Copyright 1997,	http://doolittle.ica	GNU GENERAL	http://www.gnu.or
	1999, 2000, 2003	rus.com/ntpclien	PUBLIC LICENSE	g/licenses/old-lice
	Larry Doolittle	t/ntpclient_2003	Version 2	nses/gpl-2.0.html
		_194.tar.gz		
net-snmp	Copyright(c)	http://prdownloa	GNU GENERAL	http://www.gnu.or
	2001-2003,	ds.sourceforge.n	PUBLIC LICENSE	g/licenses/old-lice
	Networks	et/net-snmp/net-	Version 2	nses/gpl-2.0.html
	Associates	snmp-5.4.1.tar.gz		
	Technology, Inc			
	All rights reserved.			
vsftpd	Author: Chris Evans	ftp://vsftpd.beast	GNU GENERAL	http://www.gnu.or
		s.org/users/ceva	PUBLIC LICENSE	g/licenses/old-lice
		ns/vsftpd-1.1.2.t	Version 2	nses/gpl-2.0.html
		ar.gz		
linux		ftp://ftp.kernel.or	GNU GENERAL	http://www.gnu.or
		g/pub/linux/kern	PUBLIC LICENSE	g/licenses/old-lice
		el/v2.6/linux-2.6.	Version 2	nses/gpl-2.0.html
		15.tar.bz2		

و ما ما ما م	Consider	ftp://ftp.potfiltor.o	CNILLOENEDAL	http://www.gpu.or
iptables	Copyright	ftp://ftp.netfilter.o	GNU GENERAL	http://www.gnu.or
	2000-2004 netfilter	rg/pub/iptables/i	PUBLIC LICENSE	g/licenses/old-lice
	project	ptables-1.3.6.tar.	Version 2	nses/gpl-2.0.html
	http://www.netfilter.o	bz2		
	rg/			
openssl	Copyright (c)	http://www.open	GNU GENERAL	http://www.gnu.or
	1998-2008 The	ssl.org/source/o	PUBLIC LICENSE	g/licenses/old-lice
	OpenSSL Project.	penssl-0.9.8k.tar	Version 2	nses/gpl-2.0.html
	All rights reserved.	.gz		
Igmpproxy	Copyright (C) 2005	http://sourceforg	GNU GENERAL	http://www.gnu.or
	Johnny Egeland	e.net/projects/ig	PUBLIC LICENSE	g/licenses/old-lice
	<johnny@rlo.org></johnny@rlo.org>	mpproxy/files/ig	Version 2	nses/gpl-2.0.html
		mpproxy/0.1/igm		
		pproxy-0.1.tar.gz		
		/download		
Dnrd	Copyright (C) 1998	http://sourceforg	GNU GENERAL	http://www.gnu.or
	Brad M. Garcia	e.net/projects/dn	PUBLIC LICENSE	g/licenses/old-lice
	<garsh@home.com></garsh@home.com>	rd/files/dnrd/2.12	Version 2	nses/gpl-2.0.html
		/dnrd-2.12.tar.gz		
		/download		
iproute	Stephen Hemminger	http://developer.	GNU GENERAL	http://www.gnu.or
	shemminger@osdl.	osdl.org/dev/ipro	PUBLIC LICENSE	g/licenses/old-lice
	org	ute2	Version 2	nses/gpl-2.0.html
	Alexey Kuznetsov			
	kuznet@ms2.inr.ac.ru			
Pppd	Paul Mackerras	ftp://ftp.samba.or		
	<paulus@linuxcare.< td=""><td>g/pub/ppp/</td><td></td><td></td></paulus@linuxcare.<>	g/pub/ppp/		
	com>			